AMENDMENTS TO THE SPECIFICATION

At the top of page 4, lines 1-14, please replace the first paragraph with the following amended paragraph:

peer); a compression method; a cipher spec (the bulk data encryption algorithm (such as null, DES, etc.) and a MAC algorithm (such as MD5 or SHA)); a master secret (a 48-byte secret shared between the client and server); an "is resumable" flag (indicating whether the session can be used to initiate new connections). The connection state includes the following elements: server and client random byte sequences that are chosen by the server and client for each connection; server write MAC secret used in MAC operations on data written by the server; client write MAC secret used in MAC operations on data written by the client; a server write key; a client write key; initialization vectors maintained for each key and initialized by the SSL handshake protocol; and sequence numbers maintained by each~~aeh~~ party for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero.

On page 4, lines 15-22, please replace the first full paragraph with the following amended paragraph:

When a number of Web clients are connecting to a particular Web site having a number of servers, each server will be required to handle a number of clients in the secure transaction environment. As a result, the processing overhead that is required by each server to perform to the secure sockets layer encryption and decryption is very high. If this were the only solution to providing secure communications protocols between the client and server, each transactional Web site would be required to provide a~~an~~ large number of servers to handle ~~to~~ the expected traffic.

Please replace the first paragraph on the top of page 11, lines 1-8, with the following amended paragraph:

or more of the processors dedicated to one or more specific tasks, such as performing the SSL encryption and decryption needed to implement the present invention. One such device which is optimal for performing the method of the present invention is described U.S. Patent Number 6,838,808 ~~in co-pending patent application serial no. __________ [NEXSI-01020USO] entitled MULTI-PROCESSOR SYSTEM, filed July 6, 2001~~. It will be recognized that any number of hardware configurations are available to implement the system and method of the present invention.

On page 11, lines 9-14, please replace the first full paragraph with the following amended paragraph:

Figure 4 illustrates the typical ~~TCI/IP~~ TCP/IP handshake sequence. The "threeway handshake" is the procedure used to establish a TCP/IP connection. This procedure normally is initiated by one TCP device (in Figure 3, the client) and responded to by another TCP device (in Figure 3, the server). The procedure also works if two TCP simultaneously initiate the procedure.